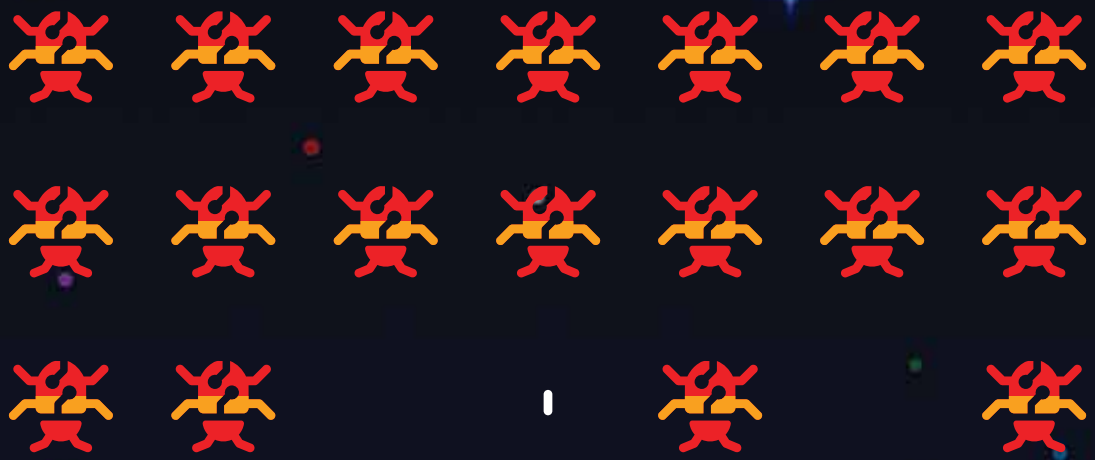
VOL
003

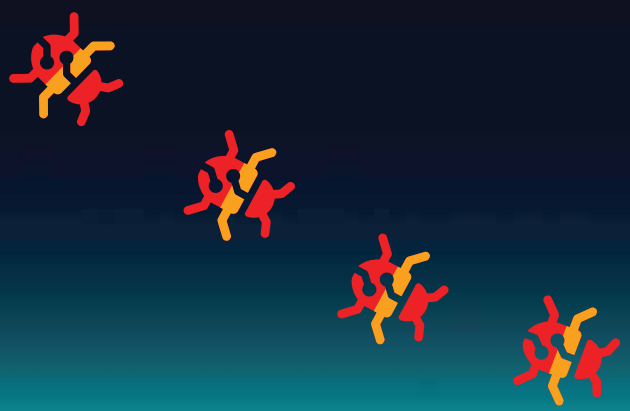
ONE STEP SECURE IT
6232271997

YEAR
2026



THE LATEST BYTE

LEVEL UP YOUR DEFENSES



onestep
Secure IT Services

THE RULES ARE EVOLVING

AI is reshaping how businesses operate and how they need to defend themselves. The terrain has shifted. The tools that power innovation also create new vulnerabilities, and the risks are real but manageable.

The difference between thriving and stumbling is how you integrate AI securely into your operations. Employees are already using AI every day. Now, business leaders are asking how to use AI responsibly, with the right safeguards in place.

Secure AI use isn't a limitation. It's a competitive advantage. Level up your defenses, and you level up your business.

ABOUT US

One Step Secure IT is an outsourced IT and cybersecurity company with over four decades protecting our customer's data from breaches to alleviate the dread of cyber attacks, costly downtime, and loss of customer trust.

OUR EXPERTISE INCLUDES

- CYBERSECURITY SERVICES
- MANAGED/CO-MANAGED IT SERVICES
- INFORMATION SECURITY SERVICES
- COMPLIANCE SERVICES

Meet Us on the Road to Power Up Your Security

ARIZONA TECHNOLOGY SUMMIT

August 25th | Grand Hyatt Scottsdale Resort

Booth #501 | Waive the $149 registration fee with promo code: ATS26OSS

CALIFORNIA TECHNOLOGY SUMMIT

October 7th | Sheraton Park Hotel at the Anaheim Resort | Waive the $149 registration fee with promo code: CTS26OSS

LEVEL UP

Why IT Alone Won't Win in the Cybersecurity Fight

You're at the arcade. You've got a fighter on screen with two totally different power-ups: one that keeps your character moving fast, and one that keeps your character from getting knocked out. Speed doesn't stop a hit. Armor doesn't make you faster. You need both of the power-ups, and not knowing how to use them is how players lose.

Now swap that fighter for your business.

Most companies have invested heavily in one power-up: Information Technology, or IT. It's the IT team (internal or outsourced) that keeps your email running, your Wi-Fi connected, and your printer from jamming on a Monday morning.

What most companies haven't realized is that this power-up doesn't automatically include the second one: Information Security, or IS. Nowadays, showing up to the boss fight with only half your gear is a losing strategy.

IT and IS are Not the Same Character Class

Think of IT as your "speed" stat. Its job is uptime and efficiency, making sure your systems work when your employees need them. IT professionals keep the lights on.

Information Security is your "defense" stat. Its job is to stop unauthorized people from getting into your systems, stealing your data, or shutting you down. Where IT asks "Does it work?", IS asks "Can someone break it?" A completely different mindset, skillset, and daily job.

Here's the part that catches business owners off guard: most IT professionals have never received formal cybersecurity training. That doesn't make them bad at their jobs. It means their job was never designed to include security in the first place.

The Gap You Can't See Until It's Too Late

When leadership asks, “Are we protected?” and the IT team says, “We're good,” the IT team could be confident in that answer. But it might be confidence built on the wrong expertise. IT teams are excellent judges of whether systems are running. They are not always equipped to judge whether those systems are defensible against a determined attacker.

This gap is exactly where breaches happen. Cyber criminals use ransomware, phishing, and other tactics to target any vulnerable system. They find unlocked doors that nobody knew were open. A well- run IT department can have every machine humming along perfectly and still be one unpatched vulnerability away from a serious incident.

How to Know Who's Actually Trained for the Fight

Information Security has its own credentialing system. A few of the most respected certifications:

CISSP (Certified Information Systems Security Professional): Considered the gold standard. Requires five years of hands-on security experience across at least two specialized domains, a rigorous exam, and ongoing education to maintain. As of the end of 2025, there were roughly 191,000 CISSP holders worldwide.

CISM (Certified Information Security Manager): Focuses on building and managing an organization's overall security program from a leadership perspective.

CISA (Certified Information Systems Auditor): Focuses on evaluating whether an organization’s controls, policies, and risk practices actually hold up under scrutiny.

If your provider can point to certifications like these, that’s a meaningful signal. If the honest answer is “no formal security training, but we’re careful,” that’s useful information too, but it signals a gap worth closing.

Four Things a Security Program Actually Does

A trained security expert isn’t just running antivirus software. Their job centers on four core objectives:

1. Keeping the business operating, even during and after an attempted attack.
2. Making sure your applications run safely, not just that they run.
3. Protecting the data you collect from customers, employees, and vendors.
4. Safeguarding the technology itself from tampering or compromise.

None of these is IT’s core mission. It’s just a reminder that these are two different jobs wearing similar-sounding titles.

Leveling Up: Practical Next Moves

Here are some important questions to ask yourself:

1. Does anyone on our team hold a recognized security certification (CISSP, CISM, CISA, etc.)?
2. Has anyone conducted a thorough risk assessment of our systems, not just a system check?
3. If we were hit with ransomware tomorrow, do we know exactly what happens next? Do we have an Incident Response Plan?
4. Are IT and IS treated as one conversation or two separate ones?

If those answers feel shaky, you’re not alone. Most businesses discover this gap only after an incident. The ones who level up early are the ones who go looking for the gap on their own terms.

Ready Player One?

You wouldn't walk into the final boss fight with half your gear equipped. Talk to a cybersecurity expert about where your defenses actually stand before something forces the question for you.

Is Your Business's AI Use Creating a Legal Liability?

By Scott Kreisberg,
Founder & CEO of One Step Secure IT

I run an IT and cybersecurity company

so data protection is literally my job. I've watched how quickly AI tools have become woven into everyday business operations and how quietly the risks have been building underneath the surface.

Most business leaders I talk to are using AI tools such as ChatGPT to draft emails, summarize their documents, brainstorm ideas, or even analyze financials.

And why wouldn't they?

These tools are fast, impressive, and genuinely useful. But there's a conversation we need to have about where your data goes when you use these tools and what a recent federal court ruling means for businesses that haven't been paying close attention.

The "Wild West" Era of AI Is Coming to an End

Every time a significant new technology enters the marketplace, it outpaces the rules designed to govern it. We saw it with social media. And now we're living it with artificial intelligence.

For the past few years, AI tools have existed in a regulatory gray zone. Businesses adopted them freely, often without policies, without training, and without much thought about the risks. That's understandable. The AI- powered tools were new, the upside was obvious, and the guardrails simply hadn't been built yet.

But that window is closing. AI data privacy needs to be part of your business strategy.

Courts, regulators, and government agencies are catching up, and the first major signal came in February 2026.

The Ruling Every Business Leader Should Know About

In U.S. v. Heppner (S.D.N.Y., Feb. 2026), Judge Jed S. Rakoff issued a ruling with a clear and far-reaching message: using consumer-grade AI tools to process sensitive or privileged information can strip away your legal protections.

Here's the short version of what happened: A defendant in a federal fraud case had used the public, consumer version of Anthropic's Claude AI to generate analyses. He then shared those outputs with his attorneys and claimed attorney-client privilege over the documents.

The court denied that protection for three important reasons:

1. **No confidential relationship exists with an AI tool.** Claude is not a lawyer. Sharing information with it is not the same as sharing it with your attorney.

2. **No reasonable expectation of confidentiality.** Anthropic's own privacy policy discloses that inputs and outputs may be used for model training and can be shared with third parties, including, in some cases, the government.

3. **The information was not prepared under counsel's direction.** The defendant acted independently and not at their attorney's instruction.

The bottom line: Once you type sensitive information into a consumer AI tool, that information may be legally treated as if you handed it to a third party. And in many cases, that means your legal protections around it, including privilege, work-product doctrine, and confidentiality, could be gone.

What This Means in Plain Business Terms

You don't have to be involved in a federal investigation for this ruling to matter to your business.

Courts and regulators are beginning to treat consumer AI tools the same way they treat any other external third-party processor. Think about what that means in practice.

If someone on your team is using a free or personal-account version of ChatGPT or a similar tool, the following types of information could potentially be considered disclosed to an outside party the moment it's entered:

- Confidential business strategies and internal planning documents
- Client communications and customer data
- Trade secrets and proprietary processes
- Financial information, forecasts, and accounting details

Security researchers have found that employees sometimes copy and paste sensitive company information into ChatGPT. Cyberhaven reported that sensitive data accounted for about 11% of prompts in its 2023 enterprise dataset.

Separately, Concentric AI reported that in the first half of 2025, Microsoft Copilot was able to access nearly three million confidential records per organization on average due to overshared permissions. This shows the risks are already present in many businesses.

On the consumer version of ChatGPT specifically, unless a user has manually turned off a setting buried in the privacy controls, conversations are used by default to train OpenAI's models.

If one of your employees pastes a client's contact information into ChatGPT to help draft an email, that data doesn't stay in your building.

Is Your Business's AI Use Creating a Legal Liability?

Certain industries handle sensitive, regulated, or legally protected data as a core part of how they operate. They are the first to feel the impact of rulings like Heppner, but they won't be the last.

Legal

Law firms and in-house legal teams using AI to draft documents, research cases, or summarize contracts may be inadvertently waiving attorney-client privilege on active client matters. The Heppner ruling is a direct warning shot.

Insurance

Underwriting, claims processing, and risk assessment workflows often involve sensitive personal and business information subject to both state and federal privacy laws. Pushing that data through a consumer AI tool is a compliance problem waiting to happen.

Healthcare

Providers, insurers, and healthcare administrators who process patient information through consumer AI tools risk violating HIPAA, the federal law governing protected health information. A HIPAA breach carries significant financial penalties and reputational damage.

Finance and Accounting

CPA firms, financial advisors, and accounting departments handling client financials, tax strategies, or investment data face fiduciary exposure and regulatory scrutiny when that data passes through third-party AI systems. The financial services industry is already under heavy regulatory oversight, and AI adds a new layer of risk.

Government Contractors

Businesses working with federal or state agencies are often bound by strict data handling requirements, such as CMMC (Cybersecurity Maturity Model Certification) and ITAR (International Traffic in Arms Regulations). Consumer AI tools simply do not meet those standards.

But What About Businesses Outside These Industries?

Here's the honest truth about business AI security: Regulated industries are feeling the pressure first, but no business is immune.

If your company handles any client data, the legal and regulatory trajectory points in one direction. The principles established in Heppner are technology-neutral. That means they apply wherever consumer AI tools are being used to process sensitive information, regardless of your industry.

Think about the day-to-day ways your team might be using AI right now:

- Asking ChatGPT to help write a proposal that includes a client's project details
- Using AI to analyze your company's revenue data or quarterly performance
- Summarizing internal meeting notes that include strategic plans or personnel discussions
- Generating marketing copy based on customer personas or behavioral data

Each of these scenarios could involve sensitive information flowing out of your organization and into a third-party system that you don't control, whose data practices you may not fully understand, and which now has legal precedent working against you.

The Cybersecurity Risk You May Not Be Thinking About

The legal exposure from Heppner is significant, but it's not the only risk on the table.

From a cybersecurity perspective, consumer AI tools represent a category called shadow AI, which refers to tools employees adopt without IT oversight or approval. Shadow AI is already responsible for a growing number of security incidents.

In IBM's Cost of a Data Breach Report 2025, shadow-AI–related security incidents were involved in 20% of the breaches studied.

When employees use personal or consumer AI accounts for work tasks:

- Your organization has no visibility into what data is leaving
- You have no way to enforce retention or deletion policies
- You have no audit trail if something goes wrong
- You have no contractual guarantee about how that data is stored or used

Italy's privacy regulator announced a €15 million (approximately $17.5 million) GDPR fine against OpenAI in December 2024, showing that even major AI providers can face regulatory enforcement, although the decision was later challenged in court.

The Good News: Secure AI for Businesses Is Available

None of this means you need to ban AI from your business. In fact, trying to eliminate AI use entirely is both impractical and unnecessary.

The right answer isn't less AI. It's smarter AI use.

There are enterprise-grade and business-specific AI solutions available that are built with exactly these concerns in mind. The right tools can give your team the productivity benefits of AI while keeping your data where it belongs.

Here's what to look for in a secure AI solution:

Data stays within your environment.
Your prompts and outputs are not used to train external models and are not accessible by the AI provider.

Access controls are in place.
You can define who on your team can use AI tools and for what purposes.

Audit logging is enabled.
If a question arises about what data was accessed or shared, you have a record.

Compliance alignment.
The solution is built to meet the requirements of your industry, whether that's HIPAA, financial regulations, or federal contractor standards.

Deployment is manageable.
You don't need a six-month implementation project. Solutions exist that can be operational quickly and scaled over time.

Practical Steps You Can Take Right Now

Whether or not you're ready to implement an enterprise AI solution today, there are steps you can take immediately to reduce your exposure:

1. Inventory your AI use.
Find out which AI tools your team is currently using, which accounts they're using (personal vs. business), and what types of information are being entered.

2. Review all AI data policies.
For any tool your team uses, understand whether your inputs are used for model training, how long they're retained, and who they can be shared with.

3. Create a basic AI usage policy.
Even a simple one-page document that outlines what information should never be entered into consumer AI tools gives your team clear guidance and reduces your legal risk.

4. Talk to your IT or cybersecurity partner.
If you don't have a trusted partner who understands both AI and security, that's a gap worth closing, especially as the regulatory environment continues to evolve.

5. Evaluate enterprise options.
Ask what a secure AI deployment would look like for your business. It may be more accessible and affordable than you think.

The Heppner ruling is a signal, not just a legal footnote. It marks the beginning of a more regulated, more accountable era for AI use in business, and the businesses that get ahead of it now will be in a much stronger position than those who wait.

New technology is a competitive advantage when you use it thoughtfully. The goal isn't to be afraid of AI. It's to be smart about how you bring it into your operations. That means understanding the risks, putting the right guardrails in place, and making sure the tools your team rely on every day aren't quietly creating liability you can't afford.

If you have questions about whether your current AI use puts your business at risk try **One Step Secure IT's AI Exposure & Security Snapshot**. Learn more below.

Your Employees Are Using AI. **Are You Managing It?**

Most organizations have zero visibility into AI adoption and the security risks that come with it.

67% of employees use AI without approval. Do you know what information your employees are sharing?

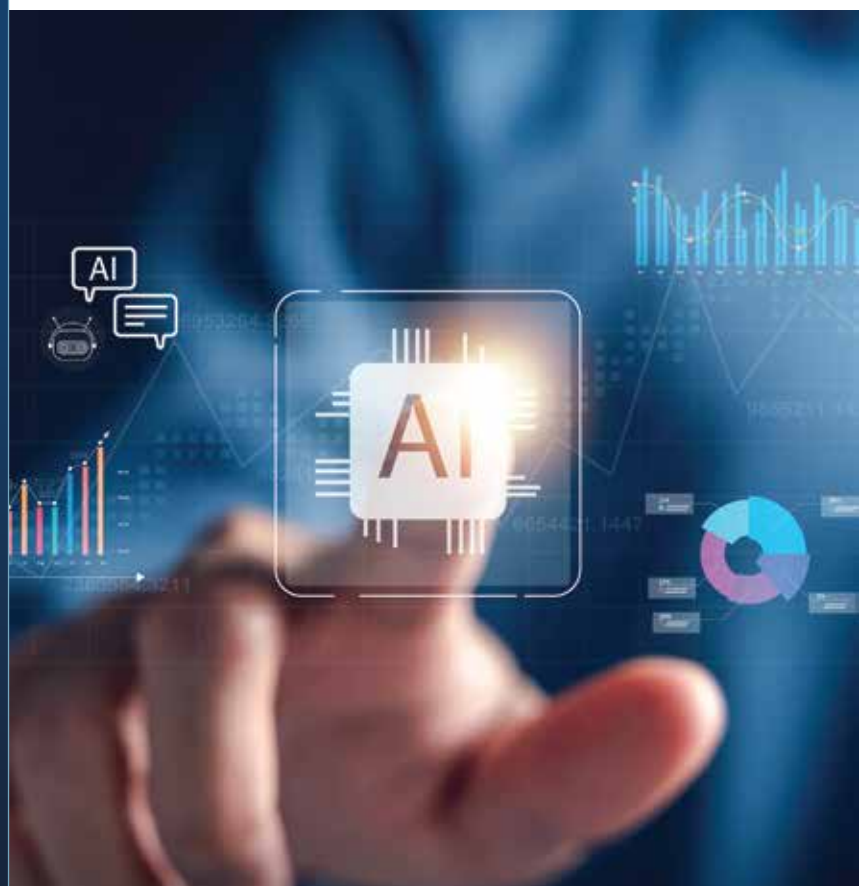
Our AI Exposure & Security Snapshot Reveals:

Data Vulnerability Scan
Where unencrypted PII & sensitive data lives

Shadow AI Discovery
What tools employees are using

Access Control Review
Identify data exposure & compliance gaps

AI Governance Audit
Policy gaps & readiness assessment



One Step Secure IT leverages Hatz AI's secure, company-managed platform, giving you full visibility and the assurance that your data never trains external models. Interested in exploring what secure AI can do for your business?

Let's talk.

Call us to schedule your **AI Exposure & Security Snapshot**. See exactly what's at risk before it becomes a breach.

623-227-1997

A Word from our Clients

They have been extremely professional, system-processed, easy to work with, and have a very high level of expertise...**They always go above and beyond, and are able to address even our most complex problems.** I have had a great experience working with them, and highly recommend them.

Denise Kozlowski
Los Angeles Business Journal

When you look at an organization like Help In Healing Home...it just makes sense to have a good IT partner to be able to ensure that your technology environment is **functional, secure, and compliant.**

John Karolzak
Help In Healing Home

We don't have to be using these one-man show companies to service our own company. **We have real cybersecurity now.**

Amanda Alquist
Alpha Overhead Doors

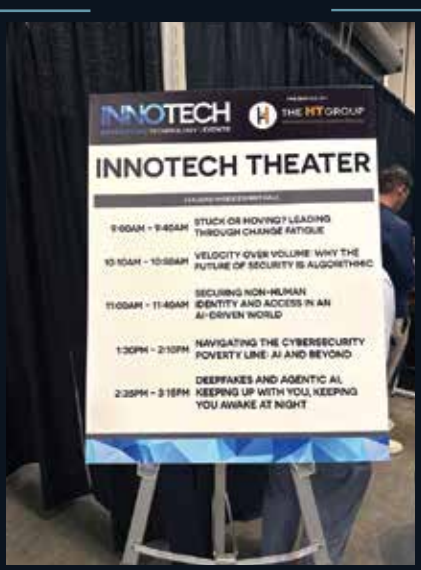
At the beginning of meeting the team, I felt very comfortable right off the bat. The staff understood my wishes. **They understood the things that made me not sleep at night.**

Rachel D. Causley
Landings Credit Union

The complexity and risks associated with security for the business outpaced our traditional IT-focused capability. We wanted a partner that could take care of our IT requests and had the skill to keep us cyber safe. **One Step is able to handle anything that comes up.**

Crista Hatfield, Hatfield Buick GMC

ONESTEP EVENT LOG



INNOTECH 2026
CONFERENCE
IN AUSTIN, TEXAS
05122026

REAL-WORLD PHISHING
PRESENTATION TO
GAMMA IOTA SIGMA -
NORTHERN ARIZONA
UNIVERSITY

INSTALLING CYBER
KNOWLEDGE
UPGRADE ■■■

One Step Secure IT
22520 North 18th Drive
Phoenix, AZ 85027

onestep
Secure IT Services

www.OneStepSecureIT.com | (623) 227-1997

Connect with us @OneStepSecureIT